REMARKS

Claims 1-48 are pending in the application. Claims 1-48 stand rejected under 35 U.S.C. 102(b).

Claim Amendments

The foregoing amendment clarifies the expression of the invention. Support for the amendment is found throughout the specification and in the original claims as detailed below. Accordingly, no new matter has been added.

Claim Rejections - 35 USC § 102

Claims 1-48 stand rejected over Elliot et al. under 35 U.S.C. 102(b). Claims 1-48 also stand rejected over Rosen under 35 U.S.C. 102(b). The rejection is respectfully traversed and reconsideration is requested. Applicant's claimed method and system for assumption by a service provider of at least one merchant function in a financial transaction between a customer and a merchant does not read on either Elliot et al. or Rosen.

Elliot et al. sought to address a problem of accommodating different security formats of smart cards of various card organizations, each having different transaction format requirements, at transaction terminals in retail stores, hotels or restaurants. (Elliot et. al, Col 1, lines 22-64). The solution proposed by Elliot et al. is a transaction terminal with an interface unit for receiving a number of modules, each of which is pre-programmed with information corresponding to transactions that can be carried out with one or more of the diverse credit or other transaction cards presented to the terminal. According to Elliot et al., the terminal allows card issuers to independently arrange and program their own security and transaction routines and to securely distribute those routines for use on a common terminal. (Elliot et al., Abstract).

To initiate a transaction on the transaction terminal of Elliot et al., an IC card is inserted into the terminal device and detected by a terminal microprocessor. The public information memory of the IC card is read by the terminal microprocessor to

obtain card data indicating the card issuing bank, type of card, and card account number. The card data is used to select one of the Elliot et al. program modules, and where such modules have multiple transaction programs, to select one of the transaction programs from the program module to be loaded into RAM for execution by the microprocessor. The selection process can be performed by polling the available modules. Once the transaction program is loaded into RAM, the control program of ROM executes a jump to a transaction program, which thereafter controls operation of the microprocessor for the remainder of the transaction. (Elliot et al., Col 8, lines 24-45).

At the beginning of the transaction program of Elliot et al., the card data read from the card is supplied to the program module. The module uses the card data and a primary key that is contained in a secret area of programmable ROM to generate a derived key which corresponds to a derived key contained on the IC card. The derived key is generated using the card data, including the card issuer information, in connection with an encryption algorithm contained in ROM or programmable ROM in the module. The terminal microprocessor sends a command to the IC card that causes the microprocessor on the IC card to generate and supply a first random number to the terminal microprocessor. This first random number is supplied to the program module, where the microprocessor executes an encryption algorithm using the derived key to encrypt the random number that is supplied. In the encryption process, neither the primary key nor the derived key are provided to the microprocessor but are retained in the program module. (Elliot et al., Col 8, line 46-Col 9, line 5).

According to Elliot et al., the first random number, which is encrypted with the derived key, is returned from the program module to the microprocessor and thereafter to the IC card. The IC card is also provided with information regarding which primary key has been used by the program module, so it can select among the derived keys in its memory and perform a decryption algorithm to obtain the identical number to the random number that it supplied to the terminal processor. The card microprocessor compares the random number that it decrypts and the random number

that it originally supplied, and if these numbers match, it is assured that the terminal to which it is connected is an authentic terminal containing the necessary primary key and encryption algorithm for the transaction. The programming on the IC card restricts its operations until it has obtained the assurance that it is dealing with an authentic terminal in order to prevent unauthorized reading or writing of information on the IC card, such as changing the authorized credit balance on the card. (Elliot et al., Col 9, lines 6-31).

Once the terminal and program module of Elliot et al. are authenticated, the terminal and program module authenticate the IC card. The terminal or module responds to the transaction program to generate a second random number. The second random number is supplied to both the program module and the card. The card uses the same derived key to decrypt the second random number and return the decrypted random number to the terminal. The decrypted random number is then provided to the program module which performs the encryption algorithm to derive a random number from the number supplied by the card in decrypted form. The program module compares the originally supplied second random number with the random number which has been decrypted and re-encrypted to assure itself that the IC card contains a proper derived key and is thus an authentic card. This process requires that the card contain only the inverse encryption algorithm and that the module contain only the encryption algorithm, thereby providing increased security so that one card cannot be used to fraudulently operate and modify another card.

After authenticating the card, the Elliot et al. terminal seeks to authenticate the identity of the person who presented the card. In this respect, a personal identification number (PIN), which is known only to that person is entered in the terminal and combined with a third random number. The third random number is provided to the IC card. The program module uses the combined third random number and the entered PIN to encrypt the combination according to the derived key. The encrypted PIN plus the third random number is supplied to the card which decrypts the combination and compares the result with the combined third random number and the PIN that is stored in the IC card. Again, the IC card is arranged so the card stored

PIN is not provided in clear text form to equipment outside the IC card. The comparison in the card provides an assurance that the user is authorized and thereafter further transaction data can be entered and processed in the terminal microprocessor. As an alternate to using a PIN, the card can include biometric information for comparison to biometric information supplied by the card user to the Elliot et al. terminal. As another alternative, the card can store biographic information for comparison to biographic information input by the card user to the Elliot et al. terminal. (Elliot et al., Col 9, line 56-Col 10, line 19).

The transaction processing according to Elliot et al. is governed by the program supplied by the program module to RAM associated with the microprocessor. This program can decide which transactions can take place off-line without communications with the issuing bank's computer and which transactions should be performed on-line by checking or updating the credit balance or other information with the bank's computer. The determination of which transaction method is used depends, for example, on the remaining balance that can be read in secure form from the IC card, the number of transactions or transaction history recorded on the IC card, or the size of the present transaction. (Elliot et al., Col 10, lines 20-35).

At the end of the transaction, the terminal records transaction data in the terminal programmable ROM, or in disc or tape form for later access for billing purposes, or in a programmable memory provided on the program module. The transaction data includes the transaction amount and authentication codes that indicate that the transaction has been properly carried out and authenticated. The transaction can also be recorded on programmable ROM on the IC card. The writing of data on the ID card is performed using encryption of the data, which can be performed by the program module or a remote computer. After the recording of the transaction information, the program ends and the terminal is prepared to receive the next card for another transaction. (Elliot et al., Col 10, lines 36-57).

Rosen sought to address the inconvenience and high cost associated, for example, with automated electronic funds transfer systems, such as computerized

EFT systems, ACH systems and POS systems, that cannot be used without the banking system and/or only during business hours and/or cannot satisfy the need for an automated transaction system that provides for the transfer of universally accepted economic value outside of the banking system. (Rosen, Col 1 line 19-Col 2, line 41). Rosen's proposed solution provides an electronic monetary system using money generating devices for generating and issuing electronic money to subscribers, transaction devices of subscribers for storing the electronic money and performing money transactions with on-line systems of participating banks or exchanging electronic money in off-line transactions with other transaction devices, teller devices at issuing and correspondent banks for processing and interfacing the transaction devices, a network providing data communications to all components of the system, and a security arrangement. (Rosen, Col 3, lines 40-63).

The money generating devices, transaction devices, and teller devices of Rosen include a combination of tamper-proof computer hardware and application software modules that can be networked together with information transmitted in encrypted form, and the electronic money transmitted with digital signatures. The electronic money is an electronic representation of currency or credit that is the equivalent of bank notes and interchangeable with paper money. The issuing banks generate the electronic currency and are liable for its redemption. The issuing banks utilize existing inter-bank clearing and settling processes. The electronic money representations are fungible, universally accepted, undeniably redeemable from the issuing banks, and have the characteristics of money transactions. Each exchange of electronic money includes data identifying the particular currency, amount, issuing bank, and digital signatures. (Rosen, Col 3, line 64-Col 4, line 29).

According to Rosen, the money generator module generates electronic notes for an issuing bank, which are then transferred by a teller money module to a subscriber utilizing a transaction money module. (Col 6, line 48-52). In order to make a payment, both the payor and payee must be subscribers to the Rosen system and both must have a Rosen transaction money module. Further, both the payor and the payee must simultaneously sign on to their respective transaction money modules.

The payor directs the payor's transaction money module to make a payment, while the payee operates the payee's transaction money module so the payee's money module issues an entitlement to receive payment. A session manager of each money module establishes communications, and a session is established for transacting between the two money modules. (Col 49, lines 5-24).

Further, according to Rosen, the payor is prompted by the payor's money module to enter an amount to transfer, and the payor enters the amount to transfer to the payee, which is displayed to the payor. The amount entered is compared to the balance of electronic money stored in the payor's money to see if there are sufficient funds for the transaction. If there are sufficient funds, the payor's money module sends a message disclosing the amount of the transfer to the payee's money module, and the payee is prompted to verify the amount will be accepted by the payee. If the payee responds in the affirmative, the payee's money module sends back an acknowledgement to the payee's money module. When the acknowledgement is received, the payor's money module sends the payment to the payee's money module, and the communication link is terminated. (Col 49, line 25-Col 50, line 9).

Still further, according to Rosen, the electronic money in a subscriber's money module can be deposited at the issuing bank via the issuing bank's teller money module (Col 46, line 46-Col 47 line 61) or at a correspondent bank that is also a subscriber to the Rosen system via the correspondent bank's teller money module. (Col 47, line 64-Col 49, line 2). The teller money modules, money generator modules and banking system periodically pass transaction records to a transaction reconciliation system at each participating bank, and unmatched transactions are transferred to an investigation system. In addition, at issuing banks, deposits are aggregated by a clearing system to consolidate all deposited electronic money, including deposits from correspondent banks, for transmission to a clearing bank. At the clearing bank of Rosen, the deposit consolidation files are processed creating a single debit or credit each issuing bank's demand account, and the processed electronic money that is cleared is sent back to a money issued reconciliation system of each of the issuing banks. The money issued reconciliation system generates

accounting transactions for the money cleared, and updates a master file of all the bank's money issued. (Rosen, Col 34, line 8-Col 35, line 61).

On the other hand, Applicant's claimed invention addresses problems associated with payment methods for Internet transactions that use, for example, "electronic checks" or "electronic payment instructions" against checking or savings accounts. Currently, electronic checks replicate the flow used for paper checks, so merchants are unsure if the electronic check will be paid and therefore delay shipment of goods to customers. Further, only a handful of banks offer such services, so there is no reason for merchants to spend money and hire people to set up systems and procedures to deal with such payment methods. In Applicant's claimed invention, the service provider, using the service provider's server, assumes one or more merchant functions and becomes the merchant's representative, albeit invisible to other participants in a transaction, and provides the merchant with approved orders and appropriate credits for the transactions. The service provider's server sits between the customer's computing device and the merchant's on-line terminal and may run the merchant's website for the merchant. Thus, the customer thinks he or she is dealing with the merchant at the merchant's website, although the customer is actually dealing with the service provider's server, and the merchant is able to use its existing systems without modification or new functionality to receive transactions via the service provider's server.

Applicant's claimed method and system for assumption by the service provider of one or more merchant functions in financial transactions does not read on either of Elliot et al. or Rosen. According to Applicant's claimed invention, the service provider server receives information about the financial transaction consisting at least in part of an electronic payment order for the merchant from the customer at a customer computing device via a network. The service provider server identifies an intended recipient of the information for the merchant consisting of either the merchant's bank or the customer's bank.

If the merchant's bank is the intended recipient, the service provider server reformats the electronic payment order for the merchant's on-line terminal and sends

the reformatted payment order to the merchant's on-line terminal. At the same time, the service provider's server also endorses the electronic payment order prepares a deposit to an account of the merchant, sends the deposit with the endorsed payment order to the merchant's bank server, posts a credit for the deposit to the merchant's account, and thereafter makes details of the deposit available to the merchant. (Spec. p. 17, line 10-p. 18, line 20).

If the customer's bank is the intended recipient, the service provider server sends the electronic payment order with a request for payment to the customer's bank server. Upon receiving the payment order, the customer's bank server debits an account of the customer for the amount of the payment order, sends an ACH credit to the merchant's bank server, and sends a transaction approval to the service provider's server. Upon receipt of the transaction approval, the service provider's server reformats the transaction approval for the merchant's on-line terminal and sends reformatted approval to the merchant's on-line terminal. (Spec. p. 18, line 21-p. 20, line 3).

The system of Elliot et al. is not capable of assumption by a service provider of merchants according to Applicant's claimed invention, nor does Elliot et al. offer any of the advantages of Applicant's claimed invention. Instead, the system of Elliot et al. provides a transaction terminal with modules pre-programmed to allow transactions with many different credit or other transaction cards at the same terminal and allows different card issuers to independently program their own security and transaction routines for use on the common terminal. (Elliot et al., Abstract). Likewise, the system of Rosen is not capable of assumption by the service provider of one or more merchant functions according to Applicant's claimed invention, nor does Rosen offer any of the advantages of Applicant's claimed invention. Rather, in the Rosen system, a member bank utilizes a computer module to issue electronic money to member subscribers who likewise must have computer modules for storing the electronic money and performing transactions. Member banks must also have computer modules for interfacing to member subscribers' computer modules and with one another. (Col. 3, lines 40-59).

Elliot et al. and/or Rosen neither disclose nor suggest the method and system for assumption by a service provider of at least one merchant function in a financial transaction between a customer and a merchant, according to Applicant's claimed invention.

Version With Markings to Show Changes Made

Amendments in the Claims:

In accordance with 37 C.F.R. § 1.121(c)(1)(ii), a marked up version does not have to be supplied for an added or deleted claim.

Conclusion

In view of the foregoing amendment and these remarks, each of the claims remaining in the application is in condition for immediate allowance. Accordingly, the examiner is requested to reconsider and withdraw the rejection and to pass the application to issue. The examiner is respectfully invited to telephone the undersigned at (336) 607-7318 to discuss any questions relating to the application.

Respectfully submitted,

Date: 12/10/02

John M. Harrington (Reg. No. 25,592)
for George T. Marcou (Reg. No. 33,014)

Kilpatrick Stockton LLP
607 14th Street, NW, Suite 900
Washington, DC 20005
(202) 508-5800

C0464-176080
WINLIB01:977344.1